WILLKIE FARR & GALLAGHER LLP
BENEDICT HUR (SBN 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN 246943)
sagnolucci@willkie.com
EDUARDO SANTACANA (SBN 281668)
esantacana@willkie.com
JOSHUA D. ANDERSON (SBN 312836)
jdanderson@willkie.com
TIFFANY LIN (SBN 321472)
tlin@willkie.com
DAVID D. DOAK (SBN 301319)
ddoak@willkie.com
NAIARA TOKER (SBN 346145)
ntoker@willkie.com
NADIM HOUSSAIN (SBN 335556)
nhoussain@willkie.com
HARRIS MATEEN (SBN 335593)
hmateen@willkie.com
333 Bush Street, 34th Floor
San Francisco, CA 94104
Telephone: (415) 858-7400
Facsimile: (415) 858-7599

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE I, et al., individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No. 3:23-cv-02431-VC
(Consol. w/ 3:23-cv-02343-VC)

DEFENDANT GOOGLE LLC'S SUPPLEMENTAL REPLY BRIEF RE: MARCH 20, 2025 ORDER REQUESTING FURTHER BRIEFING

Ctrm: 4 – 17th Floor (San Francisco)
Before: District Judge Vince Chhabria

Consol. Complaint Filed: July 13, 2023
2nd Am. Complaint Filed: August 12, 2024

TABLE OF CONTENTS

Page

I. Introduction

The Court requested supplemental briefing on whether the Second Amended Complaint ("SAC") "adequately alleged that Google has obtained [Plaintiffs'] private health information in a way that enables Google to actually identify them and link the information to them." Dkt. 191 ("Order"). In response, Plaintiffs point to only a handful of allegations in their 311-paragraph SAC and concede that there is no allegation that Signals—the only setting alleged to enable personal identification—"impact[ed] the Plaintiffs directly." Dkt. 195 at 11. Absent such allegations, the most that can be inferred from the SAC is that Google Analytics worked as designed—it does not track or exploit private health information.

Plaintiffs' authorities interpreting "health information" outside a particular contract and their recycled, out-of-district cases do not change this conclusion. Plaintiffs concede that a reasonable user would understand the Privacy Policy's language regarding "health information" to concern the use of Google's health-related features, which no Plaintiff used. Yet Plaintiffs also urge this Court to ignore this clear language and interpret "health information" based on authorities interpreting similar terms in a different, irrelevant contexts. Nothing in the SAC or Privacy Policy supports an inference that Plaintiffs' use of third party website constitutes their "using Google services that offer health-related features, such as the Google Health Studies app."

Plaintiffs also seek reconsideration of the Court's finding that the required intent is to collect "communications about private health information that Google can link to a particular, identifiable individual." Order at 4. Plaintiffs offer nothing new to resist this recitation of binding authority, and their failure to plausibly allege this intent undermines all remaining claims.

II. Plaintiffs fail to plausibly allege that actual health information was sent to Google.

Google's supplemental brief explicates the sole paragraphs Plaintiffs and the Court relied on to suggest that GA received actual health information, as opposed to routine browsing information that does not convey health information under any reasonable meaning of the term. Dkt. 194 at 3-4. Plaintiffs offer no response, much less engage with the paragraphs of the SAC Google identified. This alone justifies dismissal with prejudice. It remains completely unclear what

actual health information Plaintiffs allege snuck into the data pipeline, whether or not identifiable or intentional. The closest Plaintiffs come in the reams of an inadmissible attachment is that a user clicked a "Schedule Appointment" button on an unauthenticated webpage that leads to a phone number and otherwise reveals nothing about the user's health. The Court should not set the standard that such an anodyne piece of browsing information constitutes health information.

III. Plaintiffs admit their claim of "identifiability" relies either on optional features they cannot allege were enabled, or semantics that render all information "identifiable."

Plaintiffs still fail to explain how the SAC alleges that the *gid* cookie actually operated in an identifiable way (i.e., by pleading activation of the Signals feature). Nor do they allege that *cid* cookies tie pseudonymous identifiers to personally identifiable information. Plaintiffs instead invoke broad definitions and theoretical capabilities that the Court already deemed insufficient to support an inference that Google *in fact* collected private health information in an identifiable way.

A. Plaintiffs fail to show allegations regarding "*gid*" identifiability.

In their supplemental brief, Plaintiffs broadly argue that identifiability is unavoidable with GA, out of the box. But the SAC on its face alleges that *any* identity linkage performed with the *gid* cookie *requires* both the developer's activation of Signals (a non-default feature) and user consent to Ads Personalization. *See* Dkt. 194 at 6–7 (citing SAC ¶¶ 97, 105). And Plaintiffs admit "there are no allegations or evidence either way" as to whether Signals was actually in use by a healthcare entity, or whether any Plaintiff opted into Ads Personalization. *See* Dkt. 195 at 11. The paragraphs they cite to insinuate a supposed "misunderstanding" of their allegations are the same ones Google identified, none of which support an inference that the *gid* cookie sends identifiable information by default. *Compare* Pl.'s Resp. Br., ECF 195 at 8 (discussing SAC ¶¶ 85, 91–104), 11 (quoting SAC para. 105, which discusses Signals) *with* Google's Resp. Br., ECF 194 at 5–7.

Plaintiffs then argue that because Google "*could*" associate data with account holders via Google Signals, the *gid* cookie data must therefore be *capable* of personal identification. *See id.* (emphasis added). In other words, they argue rhetorically, how else could Google effectuate the Signals feature but by having the means to identify individual users?

That inference stretches *Twombly* past breaking; indeed, *Twombly* rejected such conjecture and conspiracy theory. *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007). The facts as alleged are that when Signals is on, Google may identify; when it is off, Google does not. How Google accomplishes this isn't particularly relevant. Further, as this Court previously held, the mere fact that Google *could* personally identify users if the facts were different does not mean that it *did*, nor that it intended to. *See Doe I v. Google LLC*, 741 F. Supp. 3d 828, 840–42 (N.D. Cal. 2024). The Court's inquiry thus correctly focuses on whether the SAC adequately alleges Google obtained health information "in a way that enables Google to *actually* identify them and link the information to them," not theoretically. Order at 1 (emphasis added).

Next, Plaintiffs argue that *any data collected via any Google cookies—including pseudonymous cookies*—is "identifiable" even "before [it was] linked to information about offline identity through Google Signals." Dkt. 195 at 10. In other words, Plaintiffs semantically twist the word "identifiable" to cover their desired outcome. Plaintiffs' wordplay fails, however, because the SAC does not plausibly allege any transmission of data satisfying any legally reasonable definition of "individually identifiable information." Google offered HHS guidance and case law requiring more than the mere transmission of pseudonymous identifiers combined with website interactions. Dkt. 194 at 3–4 (citing *Am. Hosp. Ass'n v. Becerra*, 738 F. Supp. 3d 780, 802 (N.D. Tex. 2024)); *see also* Dkt. 164 (Mot. to Dismiss) at 23 (collecting cases). Indeed, identifiers like cookies are pseudonymous by design and do not identify specific individuals without additional steps linking them to real-world identities; that's just how the Internet works. Dkt. 194, at 5 & n.5. The E.U. and California both recognize that pseudonymous identifiers are distinct from individually identifiable information. *See* Dkt. 194 at 5 n.4. If the Plaintiffs were taken at their word, even an IP address, absent any other piece of information, constitutes "identifiable" information. The Ninth Circuit plainly would not accept such an absurd, market-shaking definition.

B. Plaintiffs concede they have no allegations linking "cid" or other cookies to personal identities.

Separately, the Court noted that the SAC appeared not to allege that Google collects health

information about non-Google account holders "in an identifiable way." Order at 3. It observed that the *cid* cookie appears pseudonymous and directed Plaintiffs to identify where, if at all, the SAC shows Google linking *cid* data to non-account holders' identities. *Id.*

Plaintiffs cite no such allegations. The SAC does not explain how the *cid*—a "client ID" representing a "particular user, device, or browser instance" (SAC ¶ 97)—could be matched to a non-account holder's identity. Plaintiffs point only to a general claim of "commingl[ing]" data (SAC ¶ 106)—but offers no factual detail explaining how that purported commingling (alleged generally) applies here, nor how it identifies anyone. That data may be stored on the same server or even in the same table does not mean that the further step of cross-referencing it to identify an individual is ever taken, and the SAC does not allege that it is.

Plaintiffs also rely on a 2017 GA "charter" attached to the SAC, which references "'Online to Offline measurement at scale' for 'store visits.'" Dkt. 195 at 9 (quoting Dkt. 158-11 at 266, 268). That document, however, merely outlines a broad strategy to "grow coverage of the overall media measurement" and "drive new direct revenue" across major sales verticals such as Retail, Travel, and Healthcare. Dkt. 170 at 6. It does not discuss whether Google sought, received, or used health data, or linked such data to identities. Plaintiffs concede that "[they] did not plead that connection expressly," Dkt. 195 at 9, confirming the absence of the allegations the Court seeks.

Next, Plaintiffs invoke their expansive interpretation of HIPAA's definition of "identifiable," Dkt. 195 at 10 (citing SAC ¶ 90), but the Court already noted the absence of "an allegation that Google is able to tie the *cid* cookie to any personally identifying information." Order at 3. Citing a broad regulatory standard does not fill that *factual* gap. Indeed, the SAC does not allege that GA cookies like *_ga* and *_gcl_au*, from which it claims *cid* originates, contain personal identifiers. *See* SAC ¶ 96. By contrast, the SAC confirms the pseudonymity of *cid*, acknowledging that its "value . . . should be a random UUID." *Id.* ¶ 97.

As Google argued in its motion to dismiss, such metadata—including cookie identifiers like *cid*, IP addresses, and URLs—do not constitute individually identifiable health information (IIHI) or link browsing data to a person's identity without additional allegations showing such

linkage. *See* Dkt. 164 at 23 (citing, *inter alia*, *Kurowski v. Rush Sys. for Health*, 2024 WL 3455020, at *2 (N.D. Ill. July 18, 2024) (*Kurowski II*), *Hartley v. Univ. of Chi. Med. Ctr.*, 2023 WL 7386060, at *2 (N.D. Ill. Nov. 8, 2023), which found pseudonymous metadata insufficient for IIHI under HIPAA). Plaintiffs identify no facts showing that *cid*'s "random UUID" values for non-account holders could be transformed from pseudonymous data into information identifying a real person.

IV. The SAC fails plausibly to allege that Google breached a contractual promise.

Despite conceding that "Health Information" in Google's Privacy Policy relates to the use of Google's health-related features, Dkt. 169 (Opp. to Mot. to Dismiss) at 20, Plaintiffs continue to focus on what they call the "standard definition" of "Health Information," arguing that a reasonable person would conclude that the health-related features described in the Privacy Policy encompass unrelated third-party websites that use GA. Dkt. 195 at 11-13. But Plaintiffs do not address the Privacy Policy's text or rebut Google's argument explaining why the language Plaintiffs rely on has nothing to do with this case. Nor do they address the actually relevant language: a statement about whether Google will use health information it receives from third parties to target advertising. Plaintiffs' silence on this point is no mistake.

Instead, Plaintiffs cite to a variety of non-contract cases as evidence that Google made and breached a promise in this case. Plaintiffs' extended discussion of these cases is completely beside the point.[1] A breach claim only goes so far as the contract provision on which it depends, and Plaintiffs have none to rely upon. Whatever language was at issue in other cases is irrelevant here. *See Wolf v. Superior Court*, 114 Cal.App.4th 1343, 1353–54 (2004) (rejecting the relevance of case law interpreting a term in a different contractual context).

Several of Plaintiffs' cases focus on what constitutes IIHI and PHI under HIPAA, not what constitutes "Health Information" within the four corners of the Privacy Policy, much less whether

[1] Google cited *Kurowski II* and *Hartley* in its Motion to Dismiss for the proposition that the data Plaintiffs allege Google received is not medical history, vital signs, or health metrics (or similar information) about an identifiable person, not for their interpretation of "Health information" in the Privacy Policy. *See* Dkt. 164 at 23. Google relied on *Cousin, Jones,* and *Hubbard* in the context of Plaintiffs' invasion of privacy claims, not breach of contract. *See id.* at 19, 21; Dkt. 170 at 12.

Plaintiffs pled sufficient facts to meet that definition. *See* Dkt. 195 at 11–13; *see also, e.g.*, *Kurowski II,* 2024 WL 3455020, at *2 (discussing HIPAA), *Cousin v. Sharp Healthcare,* 2023 WL 4484441, at *3 (S.D. Cal. July 12, 2023) (same), *Jones v. Peloton Interactive, Inc.,* 2024 WL 1123237, at *4 (S.D. Cal. Mar. 12, 2024) (discussing "record" information). And *Hubbard v. Google LLC* turned on "plus" factors beyond the facts alleged here to find that Google's conduct could be found to be highly offensive. 2024 WL 3302066, at *2, *7–8 (N.D. Cal. July 1, 2024).

The sole authority Plaintiffs cite that interpreted contractual terms actually undermines their position. *Kurowski v. Rush Sys. for Health*, 683 F. Supp. 3d 836, 851 (N.D. Ill. 2023) *(Kurowski I*). Plaintiffs correctly state that *Kurowski I* "upheld the contract claim . . . regardless of whether" the information collected constituted IIHI under HIPAA. Dkt. 195 at 11–12. This was because, in the relevant terms, "*Rush ma[de] a series of promises not to share or sell patients' personally identifiable information or their confidential health information* without their consent." *Kurowski I*, 683 F. Supp. 3d at 851 (emphasis added). The court thus ignored HIPAA because the contract did not tie the meaning of "personally identifiable information" or "confidential health information" to HIPAA. *Kurowski I* shows that a contract is interpreted according to its own terms.

The Privacy Policy said Google would not collect "medical history, vital signs and health metrics (like blood glucose levels), and other similar information" *when they use Google services designed to collect such information*. Dkt.158-14 at 19. Google also said it would not use health information to target advertising. *Id.* at 30. Plaintiffs allege no breach of these provisions.

V. Google never intended to collect identifiable health information.

A. ECPA and CIPA require intent to collect identifiable health information.

The Court previously held that Plaintiffs "failed to allege Google intentionally intercepted their personal health information." Dkt.157 at 10. Relying on *United States v. Christensen*, 828 F.3d 763, 790–91 (9th Cir. 2015), the Court's tentative Order reiterates that the required intent is the intent to collect "communications about private health information that Google can link to a particular, identifiable individual." Order at 4. Plaintiffs again resist this standard on the basis of rejected or inapplicable authorities. Plaintiffs' rehash adds nothing new and certainly does not, as

the Court instructed, point to allegations that support their position.

Plaintiffs' position that they need only allege that Google intend that websites use its technology is inconsistent with *Christensen,* as this Court held. Dkt. 157 at 7 (finding *Christensen* binding and *In re Google Assistant Priv. Litig*., 457 F. Supp. 3d 797 (N.D. Cal. 2020) inconsistent with *Christensen*). Plaintiffs also find no support in the authorities on which *Christensen* relies. *See United States v. Townsend*, 987 F.2d 927, 931 (2d Cir. 1993) (finding intent where defendant utilized recording equipment to intentionally intercept communications between two unknowing and unconsenting individuals.); *United States v. Hugh,* 533 F.3d 910, 913 (8th Cir. 2008) (finding intent where defendant's "own admissions indicate that his clear intention was to intercept communications" between two unknowing and unconsenting individuals). In both cases, the communications intercepted were the very communications the defendants intended to intercept.

Plaintiffs' position also makes no sense. They make the astonishing claim that "whether th[e] specific content also constitutes 'Health Information' relates to other aspects of the case, such as Plaintiffs' breach of contract claim," but "the subject matter and identifiability of Plaintiffs' intercepted communications should not impact" the intent analysis. Dkt. 195 at 2–3; *see also id.* at 5 (arguing that the "something more" "is the intent to engage in communications surveillance"). These sweeping statements cannot be reconciled with the unquestionably lawful uses of GA. *See* Dkt.164 at 22 (discussing HHS guidance). Intending simply that customers use Google's technology cannot be unlawful. As the First Circuit held, "inadvertent interceptions are not a basis for criminal or civil liability under the ECPA." *In re Pharmatrak, Inc*., 329 F.3d 9, 23 (1st Cir. 2003); *see also In re HIPAA Subpoena,* 961 F.3d 59, 67 (1st Cir. 2020) (holding insufficient to show intent allegations that the defendant's actions or omissions caused recordings to occur). On its face, Plaintiffs' position would bring about the absurd result that all source code providers would be criminally liable depending solely on whether the third-party implementers of the code, including non-healthcare providers, use it lawfully or unlawfully.

Plaintiffs' distinguishable, out-of-circuit authorities do not assist them. Dkt. 195 at 3–4. *Szymuszkiewicz* held that the defendant's *intentional* interception of his supervisor's emails was

sufficient even if the information in those emails did not prove valuable to him. *United States v. Szymuszkiewicz*, 622 F.3d 701, 703 (7th Cir. 2010). In *Abraham,* the court held that intent could be inferred based on "ample circumstantial evidence," including a memorandum by the official who ordered the recording system acknowledging the lines belonging to plaintiffs—local judges—were being recorded. *Abraham v. Cnty. of Greenville*, 237 F.3d 386, 392 (4th Cir. 2001)).

As this Court correctly noted, section 632's intent inquiry "is narrower and centers on whether the person intended to record a *confidential* communication." Order at 4 n.1 (emphasis in original) (citing *Rojas v. HSBC Card Servs. Inc.*, 20 Cal. App. 5th 427, 434 (2018) ("*Rojas I*");. Plaintiffs' authorities are consistent with that standard. In *Superior Court of Los Angeles County,* the court explained that the actor's intent is not isolated "from the object to which it is directed, namely the confidential communication; the two are inextricably bound together." *People v. Superior Court*, 70 Cal. 2d 123, 133 (1969). The court rejected that "the mere intent to activate a tape recorder which subsequently 'by chance' records a confidential communication is sufficient to constitute an offense," as it would produce unreasonable results inconsistent with legislative purpose. *Id*. at 132–33. "[A] necessary element of the offense . . . is *an intent to record a confidential communication*." *Id.* at 133 (emphasis in original).

Rojas II is not only distinguishable, but also undermines Plaintiffs' position. There, HSBC argued its interception was not intentional because its workplace policies banned the personal calls that were intercepted. *Rojas v. HSBC Card Servs. Inc*., 93 Cal. App. 5th 860, 877 (2023) ("*Rojas II*"). The court found this argument unsupported, however: HSBC's policy *did not* forbid all personal calls, and a supervisor *allowed* the very phone calls that were intercepted. *Id.* at 878–79. It therefore could not be said that HSBC took measures to prevent itself from recording confidential conversations. *Cf.* Order at 5. In contrast, here, Google's policies consistently prohibit the interception of identifiable health information. *See* Dkt. Nos. 165-2, 165-3, 165-5, 165-10.

B. Google's disclosures, along with other allegations, negate the intent element.

Plaintiffs assert that Google must have intended to receive patient-provider communications, linkable to an identifiable Google account holder, because hospitals used GA,

which assertedly provides third-parties across industries with a "comprehensive view of the entire customer journey." Dkt. 195 at 13–14. They ask the Court to ignore Google's 2018 and 2023 HIPAA disclosures (and the GA Terms of Use) stating the *opposite*, claiming "it is not fair to infer from its mere existence that Google *wanted* Providers to even find" these disclosures. *Id.* at 14–15. Instead of pleading facts to support this insinuation of concealment—even setting aside Rule 9(b)—Plaintiffs ask this Court to baselessly suppose that Google knowingly, willfully, or intentionally contravenes its own public commitments and product descriptions (and either conspires with or dupes healthcare providers to do so)—despite no alleged benefit to Google.

The SAC does not support these insinuations with facts. It does not allege that GA is designed, out-of-the-box, to collect health information. Dkt.194 at 10. Indeed, Google's policies reinforce that Google prohibits customers from providing such data. *See* Dkts. 165-2, 165-3, 165-5, 165-10. That it may have been "obvious" that hospitals would use GA does not mean Google knew, much less intended, that providers would violate their own HIPAA obligations and Google's policies by misusing it. *See* Dkt.194 at 10–11. Even so, there are no allegations that hospitals actually misused GA or transmitted actual health information.[2] The misuse of GA, contrary users' HIPAA obligations and Google's policies, cannot be what Google intended. This Court correctly concluded that Rule 9(b) governs such accusations, and Plaintiffs failed to meet it. Order at 5.

These facts offer no place for the "natural consequences" standard Plaintiffs pull from *Stumm v. Town of Pittsboro*, 355 F. Supp. 3d 751, 763 (S.D. Ind. 2018). Dkt. 195 at 13. In *Stumm*, the defendant installed lobby cameras capable of capturing audio from an adjoining room when the door was open. *Stumm*, 355 F. Supp. 3d at 754–55. The defendant ensured the cameras would shut off when the door was closed, but never tested them with the door open. *Id.* at 763. The court found that a jury could conclude the defendant intended to intercept conversations in the adjoining

[2] Plaintiffs do not dispute that Exhibits 1 and 2 were taken from expert-generated reports, which is improper under Federal Rule of Civil Procedure 10(c). *Yuan v. Facebook, Inc.*, 2021 WL 4503105, at *2 (N.D. Cal. Sept. 30, 2021) (holding that expert reports generated for litigation are not "written instruments" under Rule 10(c)). There is no authority that "facts" generated by experts are treated any differently. Nor should they be. See Dkt. 164 at 9 n.2.

room when the door was open. *Id*. Here, in contrast, Google *prohibits* customers from sending the communications Plaintiffs claim Google intends to intercept. And no facts alleged in the SAC show that Google uses or otherwise benefits from receiving such communications.

Gladstone is also inapposite. That court determined that a "catch-all provision" generally requiring Amazon's customers to comply with the law did not shield Amazon from CIPA liability. *See Gladstone v. Amazon Web Servs., Inc.*, 739 F. Supp. 3d 846, 860 (W.D. Wash. 2024). In contrast to Amazon's "catch-all provision" to abide by "all applicable laws regarding any Recording," the GA Terms expressly prohibit collecting identifiable information, and Google's HIPAA disclosures specifically warn customers not to use GA on any page that may be covered by HIPAA or to send Google PHI. *See* Dkt. 194 at 11–14. *See* Mot. to Dismiss, *Gladstone*, Case No. 2:23-cv-00491-TL, Dkt. 21 at 5 (W.D. Wash Oct. 10, 2023). Further, the product at issue in *Gladstone* was *designed* to collect confidential information (albeit with consent).

Putting aside these factual distinctions, *Gladstone* relied on a single Washington case that addressed the pre-collection duties under the Illinois Biometric Information Privacy Act (BIPA), not CIPA. *See Rivera v. Amazon Web Servs., Inc.,* 2023 WL 4761481, at *10 (W.D. Wash. July 26, 2023). But BIPA imposes affirmative pre-collection written notice and disclosure duties on entities that collect biometric data. *See* 740 ILCS 14/15(a). It also covers negligent violations. 740 ILCS 14/20(a)(1). CIPA, however, imposes no such affirmative disclosure duties and applies only to *intentional* interception of confidential information. *Gladstone*'s extrapolation from BIPA was therefor misguided and inconsistent with *Christensen*. It effectively imposes an affirmative duty on manufacturers to monitor their customers' use of the product to ensure compliance—something neither the text nor intent of CIPA can support. Indeed, such ongoing monitoring would necessitate the very intrusion Plaintiffs decry. In short, this Court was correct in holding that the intent required here is the intent to collect "communications about private health information that Google can link to a particular, identifiable individual."

VI. Conclusion

The Court should dismiss the Second Amended Complaint with prejudice.

Dated: April 10, 2025

WILLKIE FARR & GALLAGHER LLP
Benedict Hur
Simona Agnolucci
Eduardo Santacana
Joshua Anderson
Tiffany Lin
David Doak
Naiara Toker
Nadim Houssain
Harris Mateen

By: */s/ Eduardo Santacana*
Eduardo Santacana

Attorneys for Defendant
GOOGLE LLC